Scan Techniques

Most of these scan times are only available to privileges users, because they send and Receive raw packets which requires root or admin access. nmap attempts to produce accurate results but keep in mind that all this results are based on packets returned by the target machine or the firewall.

---

1. In Nmap, the -sS option is used to perform a "TCP SYN Scan." When you use the -sS option, Nmap sends TCP SYN packets to the target ports and analyzes the responses received. This type of scan is also known as a "half-open scan" or "stealth scan."

The TCP SYN scan is one of the most popular and widely used scan techniques in Nmap. It works by sending a SYN packet to the target port and analyzing the response received. If the port is open, the target responds with a SYN/ACK packet. If the port is closed, the target responds with a RST (reset) packet. By analyzing these responses, Nmap can determine if a port is **open, closed, or filtered by a firewall.**

```
nmap -Ss <target>
```

Replace `` with the IP address or hostname of the target you want to scan. Nmap will perform a TCP SYN scan on the target ports and provide a report of the open, closed, and filtered ports.

It's important to note that the TCP SYN scan is considered stealthy because it does not complete the full TCP handshake, making it less likely to be detected by intrusion detection systems (IDS) or firewalls. However, some systems and networks may still log or block SYN packets, so it's important to use Nmap responsibly and with proper authorization.

---

2. In Nmap, the "-sT" option is used to perform a TCP connect scan.

A TCP connect scan is one of the most basic and common scan types in Nmap. It works by attempting to establish a full TCP connection with the target system on the specified ports. If a connection is successfully established, Nmap considers the port as open, and if the connection is refused or times out, the port is considered closed.

The "-sT" option can be used in combination with other Nmap options to customize the scan according to your requirements. For example, you can specify the target ports using the "-p" option followed by the port numbers or ranges.

Here's an example command using the "-sT" option to perform a TCP connect scan on port 80 of a target system:

```
nmap -sT -p 80 <target IP or hostname>
```

---

3. To perform a UDP scan in Nmap, you can use the "-sU" option followed by the target IP address or hostname. Here's an example command:

```
nmap -sU <target IP or hostname>
```

By default, Nmap will scan the most common UDP ports. However, you can also specify specific ports or port ranges to scan using the "-p" option. For example:

```
nmap -sU -p 53,161,123 <target IP or hostname>
```

This command will scan UDP ports 53 (DNS), 161 (SNMP), and 123 (NTP) on the target system.

Keep in mind that UDP scanning can be slower and less reliable than TCP scanning, as UDP is a connectionless protocol. Additionally, some firewalls and network security measures may filter or block UDP packets, making it more challenging to accurately determine the state of UDP port

---

4. To perform an ACK port scan using Nmap, you can use the "-sA" option followed by the target IP address or hostname. Here's an example command:

```
nmap -sA <target IP or hostname>
```

In an ACK scan, Nmap sends TCP ACK packets to the specified ports on the target system. The ACK packets are typically sent without any payload. The response received from the target system can fall into one of the following categories:

- Open/Unfiltered: If the target system responds with a TCP RST (reset) packet, it indicates that the port is open or unfiltered. This means that the port is either accepting connections or is being filtered by a firewall that silently drops packets.

- Filtered: If Nmap does not receive any response from the target system, it indicates that the port is likely filtered. This means that the port is being blocked by a firewall or other network security measures.

It's important to note that an ACK scan does not provide information about closed ports as it only focuses on identifying filtered ports. Additionally, some firewalls may respond to all packets with a TCP RST, making it difficult to determine the state of ports accurately.

---

5. A TCP Window port scan is a technique used to determine the state of TCP ports on a target system by analyzing the TCP Window size in the response packets. The TCP Window size represents the amount of data that a receiving system can accept before it needs to send an acknowledgement.

In a TCP Window port scan, Nmap sends TCP SYN packets to the target system's specified ports. These SYN packets are sent with a specific TCP Window size set in the TCP header. Nmap then analyzes the response packets to determine the state of the ports. Here's an example command to perform a TCP Window port scan using Nmap:

```
nmap -sW <target IP or hostname>
```

During the scan, Nmap sets the TCP Window size to a specific value, and based on the response received, it categorizes the ports into the following states:

- Open: If the target system responds with a TCP SYN/ACK packet, it indicates that the port is open.
- Closed: If the target system responds with a TCP RST (reset) packet, it indicates that the port is closed.
- Filtered: If Nmap does not receive any response from the target system, it indicates that the port is likely filtered or blocked by a firewall or other network security measures.

It's important to note that TCP Window scanning can be slower compared to other scanning techniques, as it relies on analyzing the TCP Window size in the response packets. Additionally, some systems may not provide accurate or consistent TCP Window size information, which could affect the reliability of the scan results.

In Nmap, host discovery and scan techniques are two different functionalities that serve distinct purposes:

1. Host Discovery:

Host discovery is the process of identifying active hosts on a network. Nmap uses various methods to determine which IP addresses are active and can respond to network traffic. Some commonly used host discovery techniques in Nmap include ICMP (ping) echo requests, TCP SYN scans, UDP probes, and ARP requests. The goal of host discovery is to create a list of live hosts that can be further analyzed or targeted for scanning.

2. Scan Techniques:

Scan techniques in Nmap refer to the different methods used to probe and gather information about open ports, services, and potential vulnerabilities on a target system. Nmap provides a wide range of scan techniques, including TCP SYN scans (-sS), TCP Connect scans (-sT), UDP scans (-sU), TCP ACK scans (-sA), and many more. Each scan technique has its own advantages and limitations, and they can be used to gather specific information about the target system, such as open ports, operating system details, service versions, and potential vulnerabilities.

In summary, host discovery is the process of identifying live hosts on a network, while scan techniques are used to gather detailed information about the open ports, services, and potential vulnerabilities on those live hosts. Host discovery is a prerequisite for scanning, as it helps determine which hosts are worth targeting with scan techniques.

Host Discovery

1. The "-sL" option in Nmap is used to perform a simple list scan. It takes a list of IP addresses or hostnames as input and displays the targets without actually scanning them. This option is useful for generating a list of hosts that can be used for further analysis or as input for other tools.

Here is an example command using the "-sL" option:

```
nmap -sL 192.168.0.0/24
```

This command will generate a list of IP addresses within the 192.168.0.0/24 subnet without actually scanning them.

---

2. The "-sn" option, also known as the "Ping Scan," is used for host discovery without performing any port scans. When you run Nmap with the "-sn" option followed by the target IP addresses or ranges, it sends ICMP echo requests (ping) to the targets to determine if they are alive or not. If a response is received, Nmap considers the host as live. However, it does not probe for open ports or gather any detailed information about services.

Here is an example command using the "-sn" option:

```
nmap -sn 192.168.0.1-254
```

This command will perform a ping scan on the IP range 192.168.0.1 to 192.168.0.254 and display a list of live hosts.

Question #1

What is Ping Scan?

Answer #1

A ping scan, also known as an ICMP echo scan or "ping sweep," is a host discovery technique in Nmap. It is used to determine which IP addresses are active and responsive on a network.

When you perform a ping scan using Nmap, it sends ICMP echo requests (ping) to the target hosts. If a response is received, it indicates that the host is up and running. If no response is received, it suggests that the host may be down or blocking ICMP traffic.

---

3. The "-Pn" option in Nmap is used to skip the host discovery phase and assume that the target hosts are online. By default, Nmap performs host discovery using various techniques like ICMP echo requests (ping), TCP SYN scans, and others to determine if a host is alive before proceeding with further scanning.

However, if you use the "-Pn" option, Nmap will skip the host discovery phase and assume that all specified target hosts are online. This option is useful when you already know that the hosts are active and you want to directly perform port scanning or other scans without wasting time on host discovery.

Here is an example command using the "-Pn" option:

```
nmap -Pn 192.168.0.1
```

In this command, Nmap will directly start scanning the IP address 192.168.0.1 without performing any host discovery checks.

It's important to note that using the "-Pn" option can lead to inaccurate results if the target hosts are actually offline or blocking the Nmap scanning probes. Therefore, it is generally recommended to perform host discovery before conducting any scanning to ensure accurate and reliable results.

---

4. In Nmap, TCP SYN discovery is a technique used to determine if a host is up and responsive by sending TCP SYN packets to a specific port. By default, Nmap uses port 80 for TCP SYN discovery.

To perform a TCP SYN discovery on port 80 using Nmap, you can use the following command:

```
nmap -PS80 <target>
```

Replace `` with the IP address or hostname of the target you want to scan.

This command tells Nmap to send TCP SYN packets to port 80 of the target host to check if it is up and responsive. If a response is received, Nmap considers the host as up.

Keep in mind that Nmap offers various host discovery techniques, and TCP SYN discovery is just one of them. Additionally, port 80 is commonly used for HTTP, so it is a good choice for checking host availability. However, you can specify a different port number if needed by replacing `80` with the desired port in the command.

---

5. In Nmap, TCP ACK discovery is a technique used to determine if a host is up and responsive by sending TCP ACK packets to a specific port. By default, Nmap uses port 80 for TCP ACK discovery.

To perform a TCP ACK discovery on port 80 using Nmap, you can use the following command:

```
nmap -PS80 <target>
```

Replace `` with the IP address or hostname of the target you want to scan.

This command tells Nmap to send TCP ACK packets to port 80 of the target host to check if it is up and responsive. If a response is received, Nmap considers the host as up.

Please note that TCP ACK discovery is just one of the host discovery techniques available in Nmap. Port 80 is commonly used for HTTP, so it is a common choice for checking host availability. However, you can specify a different port number if needed by replacing `80` with the desired port in the command.

---

6. In Nmap, UDP discovery is a technique used to determine if a host is up and responsive by sending UDP packets to a specific port. By default, Nmap does not have a specific default port for UDP discovery.

To perform UDP discovery on a specific port, such as port 40125, using Nmap, you can use the following command:

```
nmap -PU40125 <target>
```

Replace `` with the IP address or hostname of the target you want to scan.

This command tells Nmap to send UDP packets to port 40125 of the target host to check if it is up and responsive. If a response is received, Nmap considers the host as up.

Please note that UDP discovery is just one of the host discovery techniques available in Nmap. You can specify any desired port number for UDP discovery by replacing `40125` with the port number you want to use in the command.

---

7. In Nmap, ARP scanning can be used to discover hosts on a local network by sending ARP requests to all possible IP addresses within a specified range. This technique is especially useful for scanning hosts in the same subnet without the need for ICMP or TCP/UDP packets.

To perform an ARP discovery on the local network using Nmap, you can use the following command:

```
nmap -PR <target>
```

Replace `` with the IP address or CIDR notation of the local network you want to scan. For example, if your local network is `192.168.1.0/24`, you can use:

```
nmap -PR 192.168.1.0/24
```

This command tells Nmap to send ARP requests to all IP addresses in the specified range to discover active hosts on the local network.

Please note that ARP scanning requires root/administrator privileges on the scanning machine. Additionally, some network configurations or security measures may prevent ARP scanning from working properly.